

REMARKS

The Non-final Office Action, mailed February 13, 2008, considered claims 1–40. Claims 1–2, 4–8, 10–12, 14–18, 20–22, 24–28, 30–32, 34–38 and 40 were rejected under 35 U.S.C. § 102(b), as being anticipated by Network Working Groups, request for Comments 1948, "Defending Against Sequence Number Attacks", by Bellovin (May 1996) (hereinafter Bellovin). Claims 3 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bellovin, in view of McKay, U.S. Patent Pub. No. 2002/0187788 (filed Jun. 7, 2002) (hereinafter McKay). Claims 9, 19, 29 and 39 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bellovin, in view of Afek et al., U.S. Patent Pub. No. 2002/0083175 (filed Aug. 14, 2001) (hereinafter Afek). Claims 13 and 23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bellovin, in view of McKay, and further in view of Dickman et al., U.S. Patent No. 3,728,535 (filed Aug. 19, 1971) (hereinafter Dickman).¹

By this response, claims 1–2, 5, 8–9, 21–22, 25, and 28–29 are amended and claims 11–20, 31–40 are cancelled.² Claims 1–10 and 21–30 remain pending. Claims 1 and 21 are independent claims which remain at issue. Support for the amendments may be found within Specification ¶¶ 38–43 and Fig's 4–5.³

As reflected in the claims, the present invention is directed generally toward generating initial sequence numbers in communication protocols to prevent the communications from being attacked while maintaining reliable data transfers. Claim 1 recites, for instance, in combination with all the elements of the claim, a method for generating initial sequence numbers. The method includes generating an intermediate value by providing a secret and a connection identifier key including connection information to a hash function. The hash function produced an intermediate value. Further, a monotonically increasing counter takes timer input and connection rate input and produces a fixed value and a variable amount which are combined to

¹ Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

² The amendments and remarks presented herein are consistent with the information presented by telephone by patent attorney John Bacoch (reg. no. 59,890) and attorney Thomas Bonacci.

³ However, it should be noted that the present invention and claims as recited take support from the entire Specification. As such, no particular part of the Specification should be considered separately from the entirety of the Specification.

produce a random value. The random value and the intermediate value are then combined by a monotonically increasing mathematical function to produce the initial sequence number.

Claim 21 recites a computer program product embodiment of the method of claim 1

Independent claims 1 and 21 were rejected under 35 U.S.C. § 102 as being anticipated by Bellovin, Network Working Group RFC 1948, 1996. The Applicants submit that Bellovin fails to teach each and every element of the claims as they are now recited.

In particular, Bellovin fails to teach securely initializing a hash function with at least a portion of the random input key and at least a portion of the connection identifier key for determining an intermediate value. Bellovin also fails to teach creating a monotonically increasing counter for ensuring that a same connection identifier does not have data collisions from competing sequence numbers within a predetermined period of time, and for ensuring randomness of the initial sequence number on a per connection basis for preventing attacks on the local server, the counter taking both timer information and connection rate information as input. Bellovin also fails to teach incrementing the counter a fixed value based on a passage of a predetermined time period and detecting a connection rate for a local server. Bellovin also fails to teach incrementing the counter a variable amount depending upon the connection rate for local server, the increment being based upon the connection rate and combining the fixed value and the variable amount to create a random value. Bellovin also fails to teach combining the intermediate value and the random value using a monotonically increasing mathematical function to generate the initial sequence number.

Because Bellovin fails to teach each and every element of claim 1, a rejection under 35 U.S.C. § 102 would be improper and should be withdrawn. Accordingly, the Applicants respectfully request favorable reconsideration of claim 1. As claim 21 recites a computer program product embodiment of the method of claim 1, the discussion above applies equally to claim 21 and, correspondingly, the Applicants also respectfully request favorable reconsideration of claim 21.

In view of the foregoing, Applicants respectfully submit that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicants acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicants reserve the right to challenge any

of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicants specifically request that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 13th day of May, 2008.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'R. D. Nydegger', written in a cursive style.

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant
Customer No. 47973